

REMARKS

The Office Action dated October 27, 2008 has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

Claims 1-2, 4-10, 13, 22-25, 46, and 56-71 are pending in the application. Claims 1-2, 4, 6-8, 10, 22-24, 46, 56, 58-60, and 62 have been amended to more particularly point out and distinctly claim the subject matter of the invention. No new matter is believed to be added. Applicant submits the pending claims for consideration in view of the following.

Incomplete Office Action and Improper Finality

The pending Office Action is incomplete, and finality thereof improper, because the pending Office Action failed to make a *prima facie* rejection of at least claims 1, 22, 25, and 46.

On page 4, the Office Action attempted to reject claims 1-2, 4-10, 22-25, 46, and 56-71 under 35 U.S.C. § 103(a) as being unpatentable over Jennings and Peterson (RFC 3325 Internet Draft, <http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00>, May 27, 2002 (hereafter “Jennings”) in view of W. Marshall et al. (draft-ietf-sip-privacy-04txt, February 27, 2002 (hereafter “Marshall”), and further in view of 3GPP TSG SA WG3 Security – S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces (hereafter “3GPP”) in light of the knowledge of one of ordinary skill in the art. In support of this

rejection, the Office Action took the position that the rejected claims were obvious to one of ordinary skill in the art in light of the foregoing references. However, the Office Action failed to make a *prima facie* rejection under 35 U.S.C. § 103(a) for at least the reason that the Office Action failed to consider each and every limitation on the rejected claims.

MPEP 2143.03 indicates that, “**All words** in a claim must be considered in judging the patentability of that claim against the prior art” (emphasis added). Furthermore, MPEP § 2143 states that “[t]he key to supporting any rejection under 35 U.S.C. 103 is the **clear articulation** of the reason(s) why the claimed invention would have been obvious. The Supreme Court in KSR noted that the analysis supporting a rejection under 35 U.S.C. 103 should be made explicit” (emphasis added).

In violation of the foregoing requirements, the Office Action failed to consider all the features of the rejected claims. For example, the Office Action never addressed the “second layer,” which is recited twice in each of independent claims 1, 22, 25, and 46. More specifically, on pages 5-6, the Office Action attempted to set forth sufficient grounds for supporting the rejection of claim 1; however, the grounds set forth do not address the twice-recited “second layer.”

Consequently, the Office Action failed to consider all the features of the rejected claims and failed to provide a clear articulation of the reasons why the claimed invention is alleged to be obvious. Because all of the claimed features have not been explicitly considered in the record, the Office Action is not complete as to all matters, as required

by 37 C.F.R. § 1.104(b). Therefore, a new Office Action must be issued that clearly sets forth the disposition of the pending claims.

§ 112 Rejection, Second Paragraph

Claim 23 was rejected under 35 U.S.C. §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the invention. More specifically, the Office Action objected to claim 23 for reciting “security server is configured to messages via,” without antecedent basis. As indicated above, claim 23 has been amended in a manner that remedies the foregoing issues. Withdrawal of this rejection is therefore respectfully requested.

§103(a) Rejection

Claims 1-2, 4-10, 22-25, 46 and 56-71 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Jennings and Peterson (RFC 3325 Internet Draft, <http://tools.ietf.org/html/draft-ietf-sip-asserted-identity-00>, May 27, 2002 (hereafter “Jennings”) in view of W. Marshall et al. (draft-ietf-sip-privacy-04txt, February 27, 2002 (hereafter “Marshall”), and further in view of 3GPP TSG SA WG3 Security – S3#18, Proposed changes to 33.2000 about Za, Zb, Zc interfaces (hereafter “3GPP”) in light of the knowledge of one of ordinary skill in the art. The Office Action asserted that the combination of Jennings, Peterson and 3GPP disclosed all of the elements of claims 1-2, 4-10, 22-25, 46 and 56-71. This rejection is respectfully traversed as follows.

Claim 1, upon which claims 2, 4-10, 13, and 63-67 depend, is generally directed to an apparatus that includes a determiner configured to determine whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer. The apparatus also includes a forwarder configured to forward the message within said first network regardless of the result of the determination. The apparatus further includes a modifier configured to modify the message so as to include a second layer indication that the message has not been through a security check when the result of the determination is that the message has not been through a security check, wherein said second layer is a higher layer than said first layer.

Claim 22, upon which claims 23, 24 and 68 depend, is generally directed to a system that includes a security server. The system also includes a network processing element, the security server being configured to receive a message, determine whether the message has been through a security check by determining whether or not the message has been received with security at a first layer, when the result of the determination is that the message has not been through a security check modify the message so as to include a second layer indication that the message has not been through a security check, wherein said second layer is a higher layer than said first layer, and forward the message to the network processing element regardless of the result of the determination.

Claim 25, upon which claims 56-62, 69-70 and 71 depend, is generally directed to a method that includes determining that a message received at a first network has not

been through a security check by determining that the message has not been received with security at a first layer. The method also includes modifying the message so as to include a second layer indication that the message has not been through a security check, wherein the second layer is a higher layer than the first layer. The method further includes forwarding the message within the first network.

Claim 46 is generally directed to an apparatus which includes determining means for determining whether a message received at a first network has been through a security check by determining whether or not the message has been received with security at a first layer. The apparatus also includes modifying means for, when the message is determined not to have been through a security check, modifying the message to include a second layer indication that the message has not been through a security check, wherein the second layer is a higher layer than the first layer. The apparatus further includes forwarding means for forwarding the message within the telecommunications network regardless of whether the message has been through a security check.

Each of the foregoing claims recites limitations that are not disclosed or suggested by a combination of Jennings, Marshall, and 3GPP.

Jennings discusses private extensions to session initiation protocol (SIP) that enable a network of trusted SIP servers to assert the identity of end users or end systems, and the application of existing privacy mechanisms. In Jennings, the use of the extensions is only applicable inside an administrative domain with previously agreed-upon policies for generation, transport, and usage of such information.

Marshall discusses extensions to SIP that enable a network of trusted SIP servers to assert the identity of end users or end systems, and to convey indications of end-user requested privacy. Marshall discloses that the use of these extensions are only applicable inside an administrative domain, or among federations of administrative domains with previously agreed-upon policies for usage of such information.

3GPP discusses proposed changes to 33.200 about Za, Zb, and Zc interfaces. The 3GPP document addresses UMTS key management and distribution architectures for native IP based protocol. The UMTS key management and distribution architecture is based on IPsec IKE protocol.

However, a combination of Jennings, Marshall, and 3GPP fails to disclose or suggest all the limitations of the rejected claims. More specifically, a combination of Jennings, Marshall, and 3GPP fails to disclose or suggest “a determiner configured to determine...whether or not the message has been received with security at a first layer,” as recited in claim 1, and as similarly recited in claims 22, 25, and 46, though each claim has its own scope.

In Jennings, a proxy in a Trust Domain receives messages from nodes that it may or may not trust. See Jennings Section 5. On one hand, when a proxy receives a message from a node it does not trust, the proxy MUST authenticate the originator of the message, and use the identity which results from this authentication to insert an appropriate P-Asserted-Identity header field into the message. *Id.* On the other hand, if the proxy

receives a message from a node that it trusts, the proxy can use the information in the P-Asserted-Identity header field, if any, as if it had authenticated the user itself. *Id.*

However, Jennings fails to disclose determining whether a message has been received with security at a first layer. Instead, as indicated above, Jennings merely discloses that when a proxy may authenticate and modify a message based on whether or not the message come from a trusted node (See Jennings Section 5). As best understood, the “trusted domain” is defined as a pre-registered set of SIP nodes, and that a receiver of an SIP message determines whether or not the received message is from an SIP node within the trusted domain by identifying the SIP node from which the message is received by reading the received message at the SIP application layer and by determining whether said SIP node is one of said pre-registered SIP nodes. At any rate, Jennings does not disclose the node as being able to determine whether a message is received with security at a first layer.

Similarly, Marshall fails to disclose or suggest the foregoing limitations. In Marshall, when a proxy receives a message from a trusted entity, the proxy does not apply any special processing until the message is forwarded (See Marshall, Section 7.5). However, when the proxy receives a message from an untrusted entity, the proxy **MUST** examine the message for the presence of any Remote-Party-ID headers (*Id.*). Depending upon the identity of the calling party, the proxy in Marshall performs various operations such as including a calling subscriber Remote-Party-ID in the message or add an rpi-screen parameter set to “no” (*Id.*) However, similar to Jennings, Marshall fails to

disclose or suggest that the proxy is able to determine whether a message is received with security at a *first layer*. Instead, the proxy of Marshall “MUST” examine the message for the presence of any Remote-Party-ID when the message is from an untrusted entity (*Id.*).

Also similar to Jennings, 3GPP fails to disclose or suggest the limitations mentioned above. While 3GPP discloses Za-interfaces that cover secure IP communications between security domain gateways (SEGs) (See 3GPP, page 3), 3GPP does not disclose that, for example, the SEGs perform one or more operations to determine whether a message is received with security at a *first layer*. Moreover, 3GPP fails to provide any suggestion or motivation for the SEGs to do so. Instead, 3GPP merely discusses that secure tunnels may be established and used to forward secure traffic.

In light of the above, a combination of Jennings, Marshal, and 3GPP fails to disclose or suggest “a determiner configured to determine...whether or not the message has been received with security at a first layer,” as recited in claim 1, and as similarly recited in claims 22, 25, and 46, though each claim has its own scope. Consequently, a combination of Jennings, Marshal, and 3GPP fails to disclose or suggest all the limitations of the rejected claims. Similarly, combination of Jennings, Marshal, and 3GPP fails to disclose or suggest all the limitations of claims 2, 4-10, 23-24, and 56-71, for their dependency from claims 1, 22, 25, and 46, and for the patentable subject matter recited therein. Withdrawal of this rejection is therefore respectfully requested for at least these reasons.

Additionally, the rejected claims are not obvious to one of ordinary skill in the art because one skilled in the art would not have been motivated to alter Jennings with Marshall and 3GPP to arrive at the claimed invention. With respect to combining Jennings and 3GPP, one skilled in the art would not be motivated to alter Jennings with because doing so would require a contradiction of the fundamental design and operation of Jennings. As stated above, when the proxy of Jennings receives a message that is not trusted, the proxy authenticates the message using Digest authentication and then inserts the resulting P-Asserted-ID header field into the message (See Jennings, Sections 4-5). By contrast, 3GPP discusses SEGs using IKE to negotiate, establish, and maintain a secure tunnel between each other (See 3GPP, page 2). Accordingly, substituting the foregoing operations of Jennings for those of 3GPP would fundamentally frustrate the design of Jennings because, for example, Jennings is not designed to rely upon the establishment and maintenance of a secure tunnel. Rather, Jennings is directed to authenticating and modifying a message when it is received from an untrusted source. Consequently, one skilled in the art would not be motivated to combine the operations of Jennings with those of 3GPP.

Similarly, one skilled in the art would not be motivated to alter Jennings with Marshall because each document provides a separate and distinct set of operations to perform when a message is received from an untrusted source. As stated above, Jennings operates to authenticate the message using Digest authentication and inserting the resulting P-Asserted-ID header field into the message. By contrast, Marshall discloses

that the proxy “MUST” examine the message for a Remote-Party-ID header, which “MUST” each be verified or have their rpi-screen parameters set to “no.” Accordingly, substituting the foregoing operations of Marshall for those of Jennings would frustrate the design of Jennings because, for example, the message would not include a P-Asserted-ID header field. Consequently, one skilled in the art would not be motivated to combine the operations of Jennings with those of Marshal.

In light of the above, one skilled in the art would not be motivated to combine Jennings, Marshal, and 3GPP to arrive at the claimed invention for at least the reason that doing so would require a fundamental alteration of the principles upon which Jennings is directed. Therefore, the rejected claims are not obvious in view of a combination of Jennings, Marshal, and 3GPP. Withdrawal of this rejection is therefore respectfully requested for this reason as well.

Claim 13 was rejected under 35 U.S.C. §103(a) as being unpatentable over Jennings, Marshall, 3GPP, and Soininen (RFC 3574 Internet Draft, <http://tools.ietf.org/html/draft-ietf-v6ops-3gpp-cases-00>, September, 2002). The Office Action took the position that Jennings, Marshall, and 3GPP fail to disclose the features of claim 13. However, the Office Action also took the position that Soininen discloses the features of claim 13 in a manner that renders claim 13 obvious to one of ordinary skill in the art. Applicant respectfully asserts that claim 13 is not obvious.

Jennings, Marshall, and 3GPP are each discussed above with respect to claim 1. Soininen discusses different scenarios in a Third Generation Partnership Project (3GPP)

defined packet network that would need IP versions 6 and IP version 4 transitions. However, similar to Jennings, Marshall, and 3GPP, Soininen fails to disclose or suggest, “a determiner configured to determine...whether or not the message has been received with security at a first layer,” as recited in claim 1, from which claim 13 depends.

Instead, Soininen discloses scenarios where the user equipment connects to nodes in other networks, e.g., the Internet. Indeed, Soininen, similar to Jennings and Marshall, does not disclose that, for example, a determination is made as to whether or not a message has been received with security at a first layer. Accordingly, Applicant respectfully asserts that a combination of Jennings, Marshall, 3GPP, and Soininen fails to disclose or suggest all the limitations of claim 1. Additionally, Soininen fails to disclose or suggest a manner or motivation for combining Jennings, Marshall, and 3GPP, as discussed above. Therefore, Applicant respectfully requests that the rejection of claim 13 be withdrawn for the dependency of claim 13 from claim 1, and for the patentable subject matter recited therein.

Conclusion


Applicant respectfully requests that the pending rejections be withdrawn and that the pending claims promptly pass to allowance.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by

telephone, the applicant's undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, the applicant respectfully petitions for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,



Jared T. Olson
Registration No. 61,058

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

JTO:skl